Administração de dispositivo do Cisco WLC usando TACACS+

Contents

Introduction

Este documento descreve como configurar o TACACS+ para a administração de dispositivos do Cisco Wireless LAN Controller (WLC) com o Identity Service Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Identity Service Engine (ISE)
- Conhecimento básico do Cisco Wireless LAN Controller (WLC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

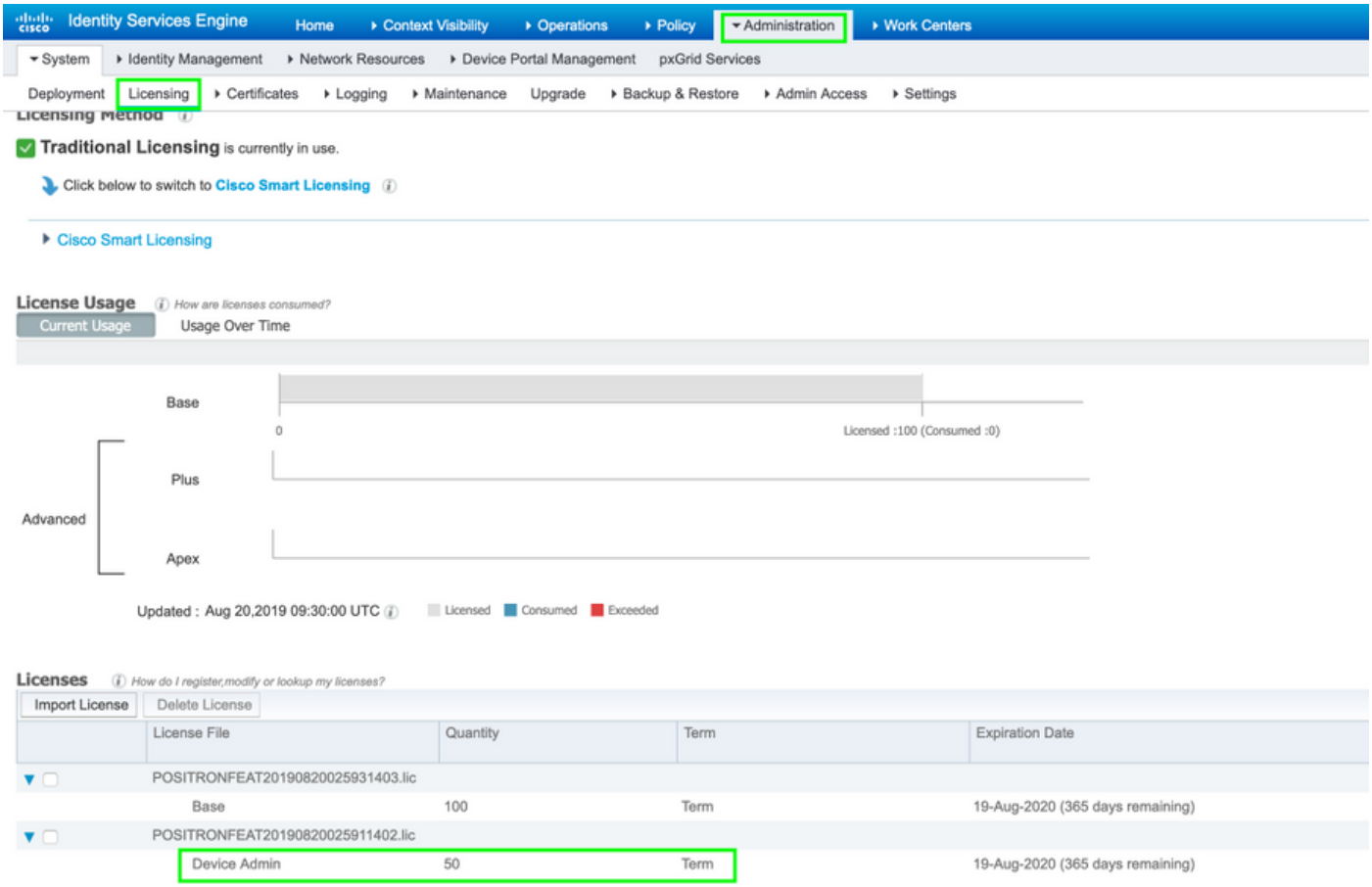
- Cisco Identity Service Engine 2.4
- Controladora de LAN sem fio Cisco 8.5.135

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuração

Etapa 1. Verifique a licença de administração do dispositivo.

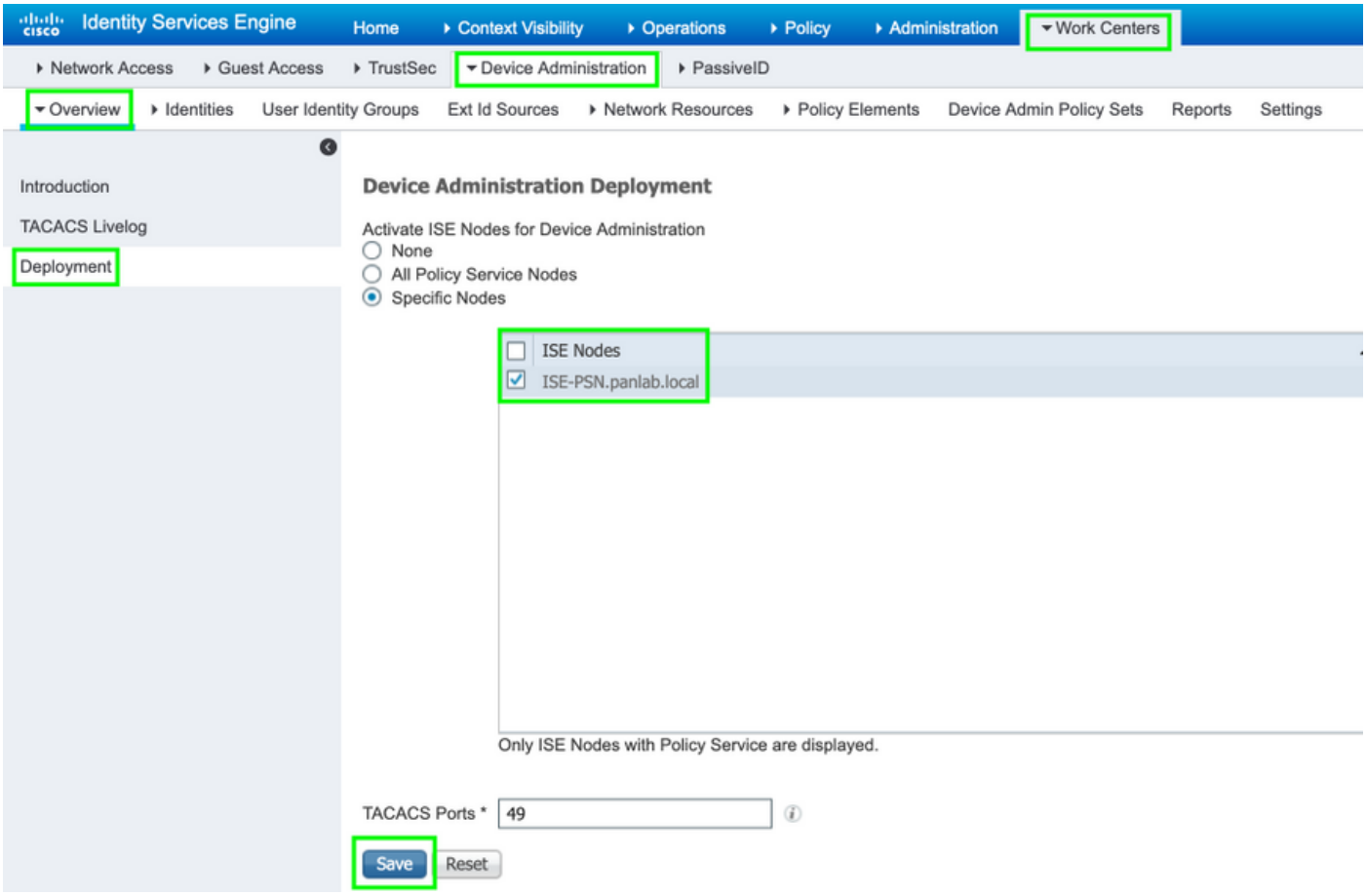
Navegue até **Administration > System > Licensing** tab e verifique se a licença do **Device Admin** está instalada, como mostrado na imagem.



Note: A licença de administrador de dispositivo é necessária para usar o recurso TACACS+ no ISE.

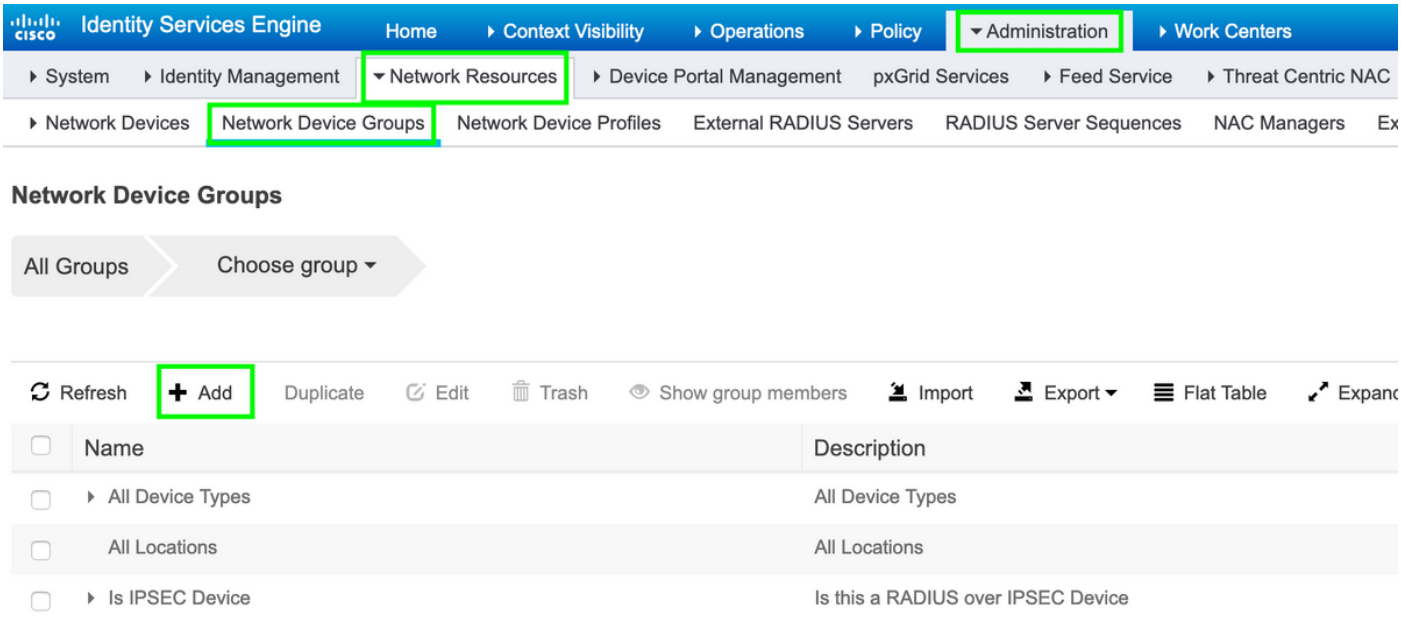
Etapa 2. Ative a administração de dispositivos em nós PSN do ISE.

Navegue até **Centros de trabalho > Administração do dispositivo > Visão geral**, clique na guia **Implantação, selecione** o botão de opção Nó PSN específico. **Ative** a Administração de dispositivos no nó ISE marcando a **caixa de seleção** e clique em **salvar**, como mostrado na imagem:



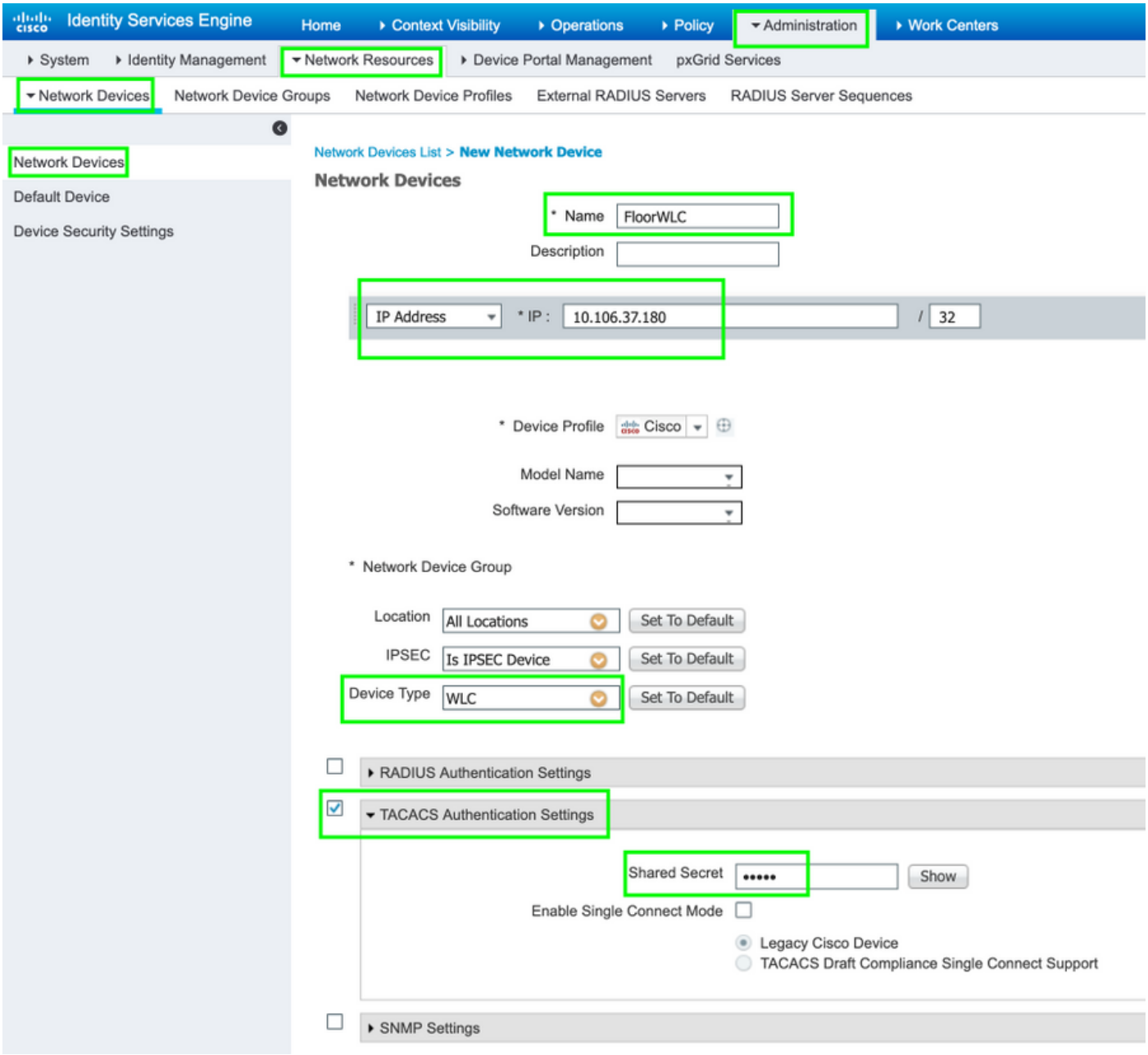
Etapa 3. Crie um grupo de dispositivos de rede.

Para adicionar a WLC como um dispositivo de rede no ISE, navegue para **Administration > Network Resources > Network Device Groups > All Device Types**, crie um **novo grupo** para a WLC, como mostrado na imagem:



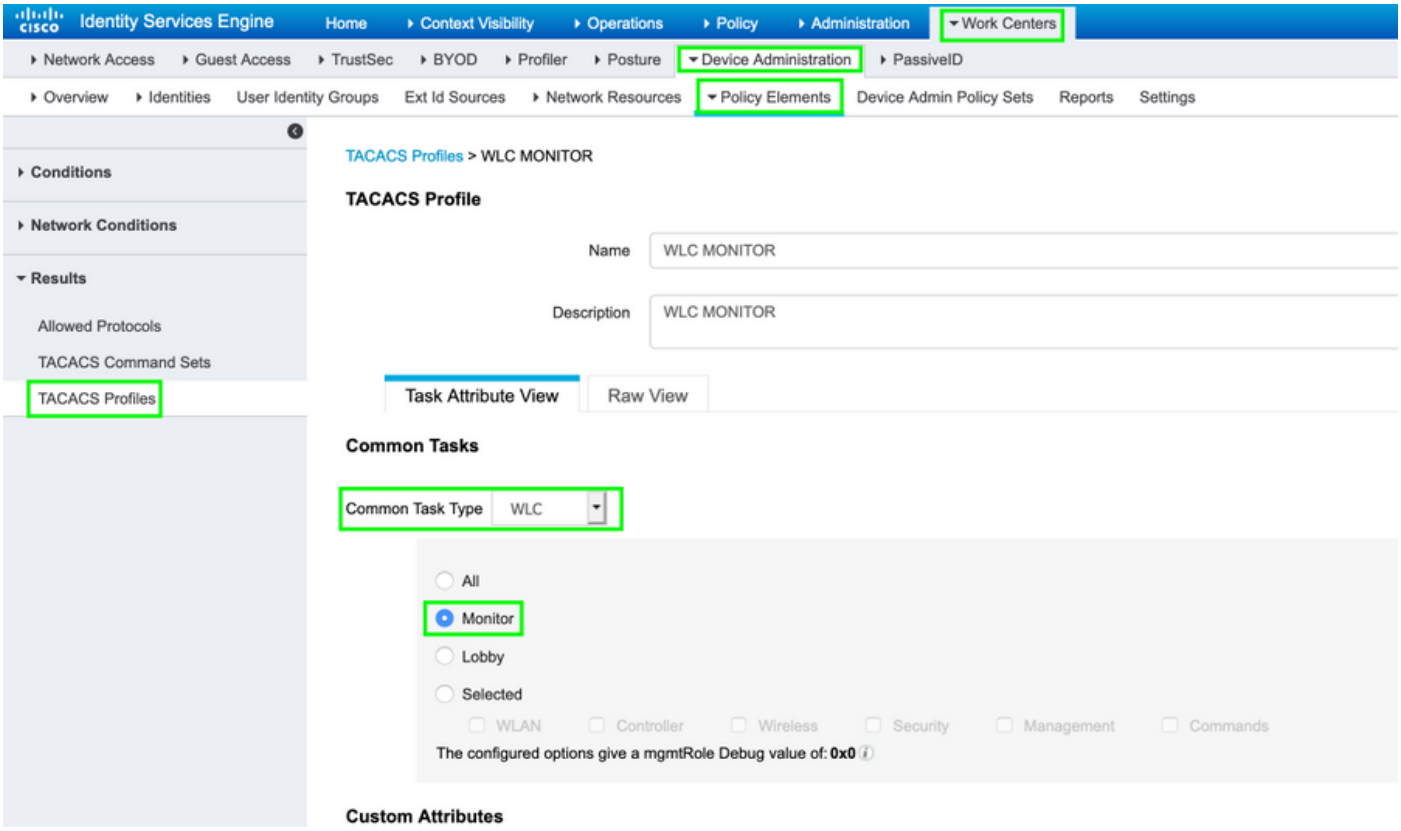
Etapa 4. Adicione a WLC como um dispositivo de rede.

Navegue até **Centros de trabalho > Administração de dispositivos > Recursos de rede > Dispositivos de rede**. Clique em Adicionar, fornecer nome, endereço IP e selecione o tipo de dispositivo como **WLC**, marque a caixa de seleção **TACACS+ Authentication Settings** e forneça a chave do **segredo compartilhado**, como mostrado na imagem:

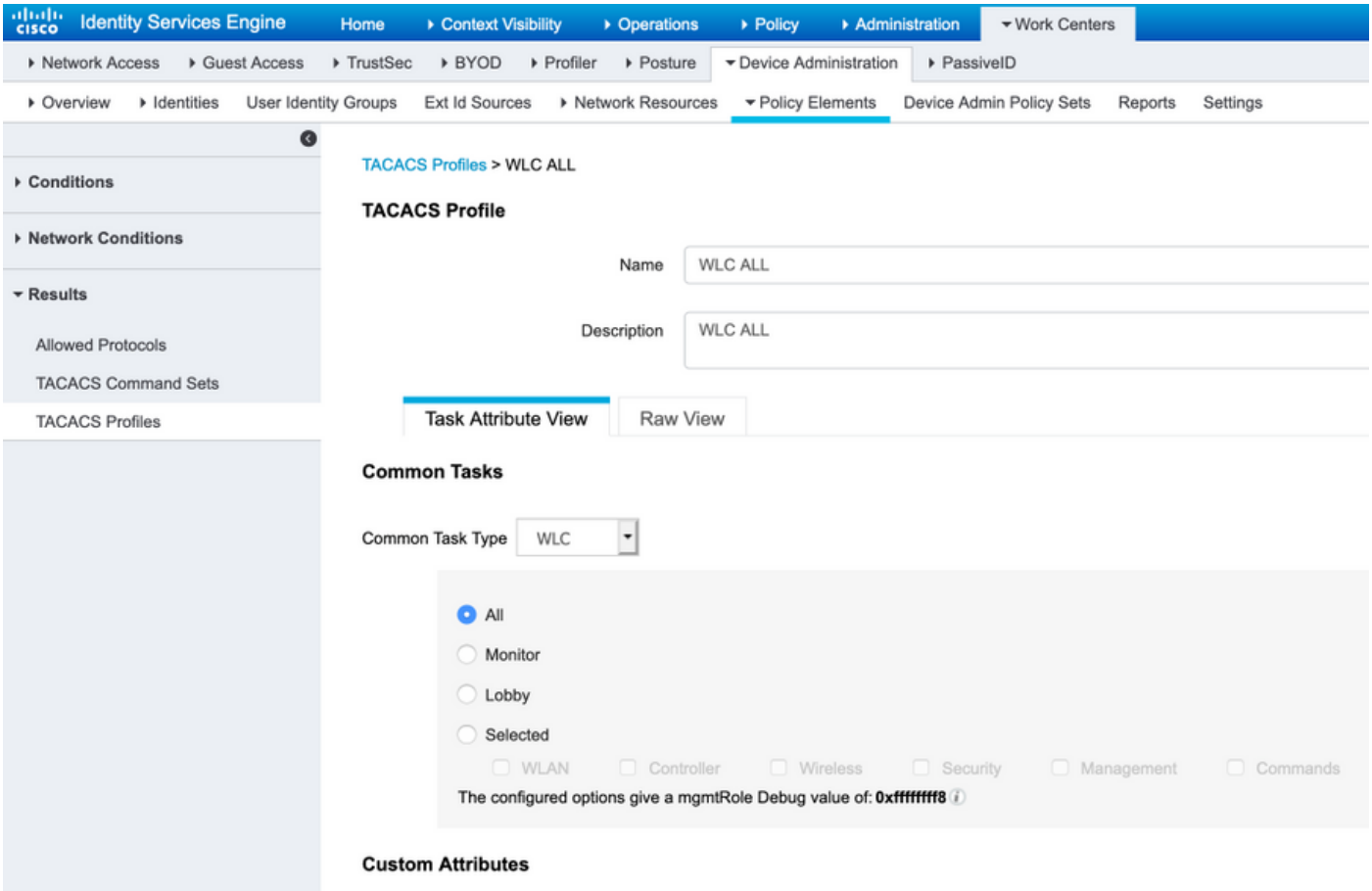


Etapa 5. Crie um perfil TACACS para WLC.

Navegue até **Centros de trabalho > Administração de dispositivos > Elementos de política > Resultados > Perfis TACACS.** Clique em **Adicionar e** forneça um **Nome.** Na guia **Exibição de atributo de tarefa**, selecione **WLC** para **Tipo de tarefa comum.** Há perfis padrão presentes a partir dos quais selecione **Monitor** para permitir acesso limitado aos usuários, como mostrado na imagem.

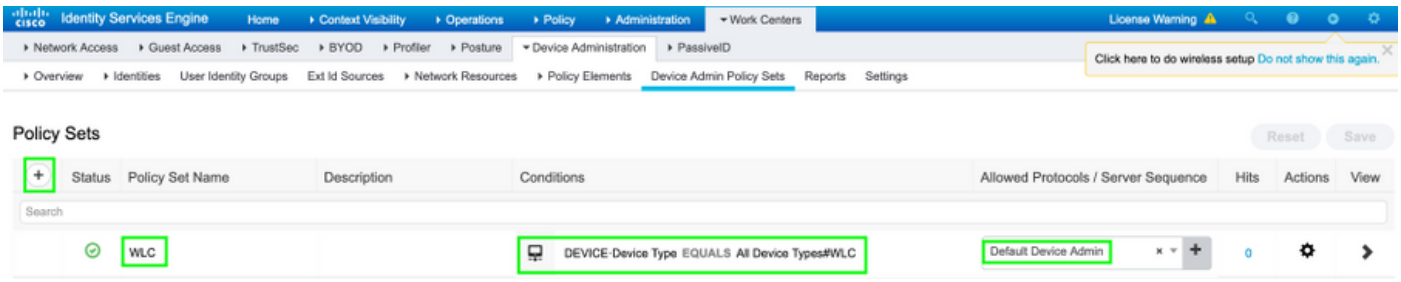


Há outro perfil padrão **All** que permite acesso total ao usuário como mostrado na imagem.



Etapa 6. Criar um Conjunto de Políticas.

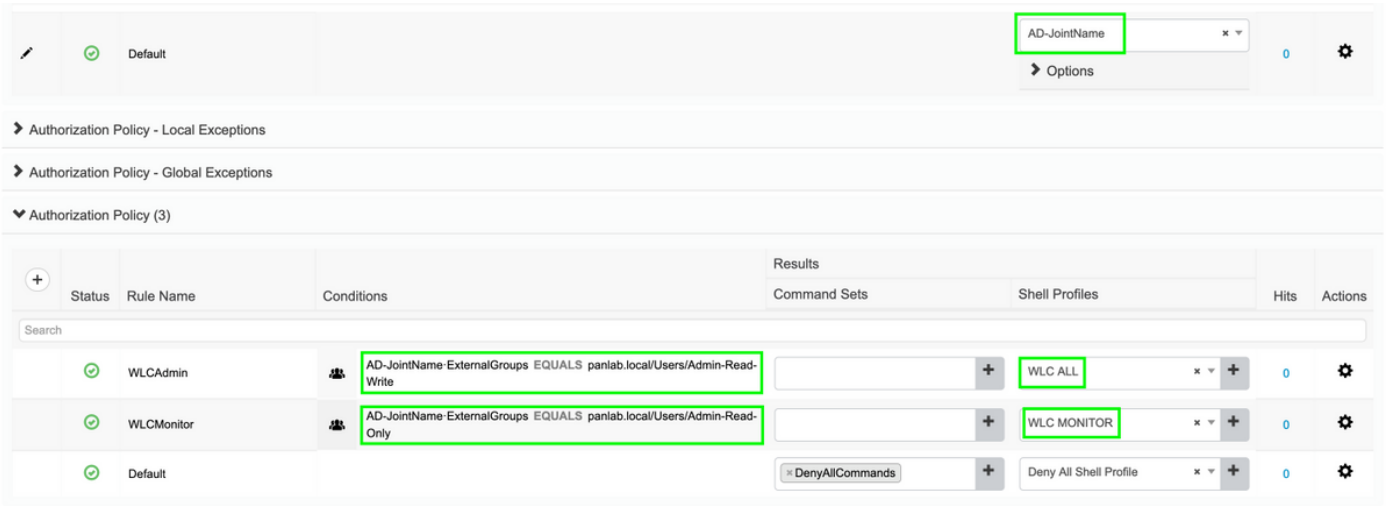
Navegue até **Centros de trabalho > Administração de dispositivos > Conjuntos de políticas de administração de dispositivos.** Clique em **(+)** e atribua um nome ao Conjunto de políticas. Na condição da política, selecione **Tipo de dispositivo** como WLC, os protocolos permitidos podem ser **Administrador de dispositivo padrão**, como mostrado na imagem.



Passo 7. Criar Políticas de Autenticação e Autorização.

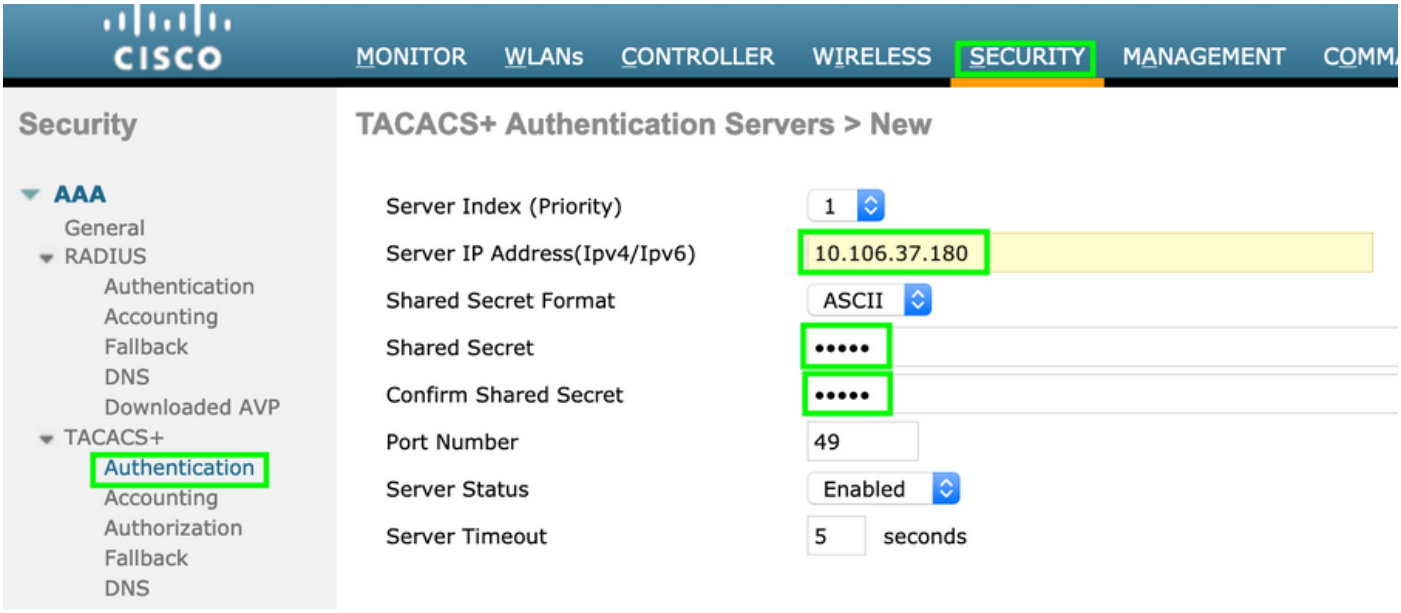
Neste documento, dois grupos de exemplo **Admin-Read-Write** e **Admin-Read-Only** são configurados no Ative Diretory e um usuário dentro de cada grupo **admin1**, **admin2** respectivamente. O Ative Diretory está integrado ao ISE por meio de um ponto de conexão chamado **AD-JointName.**

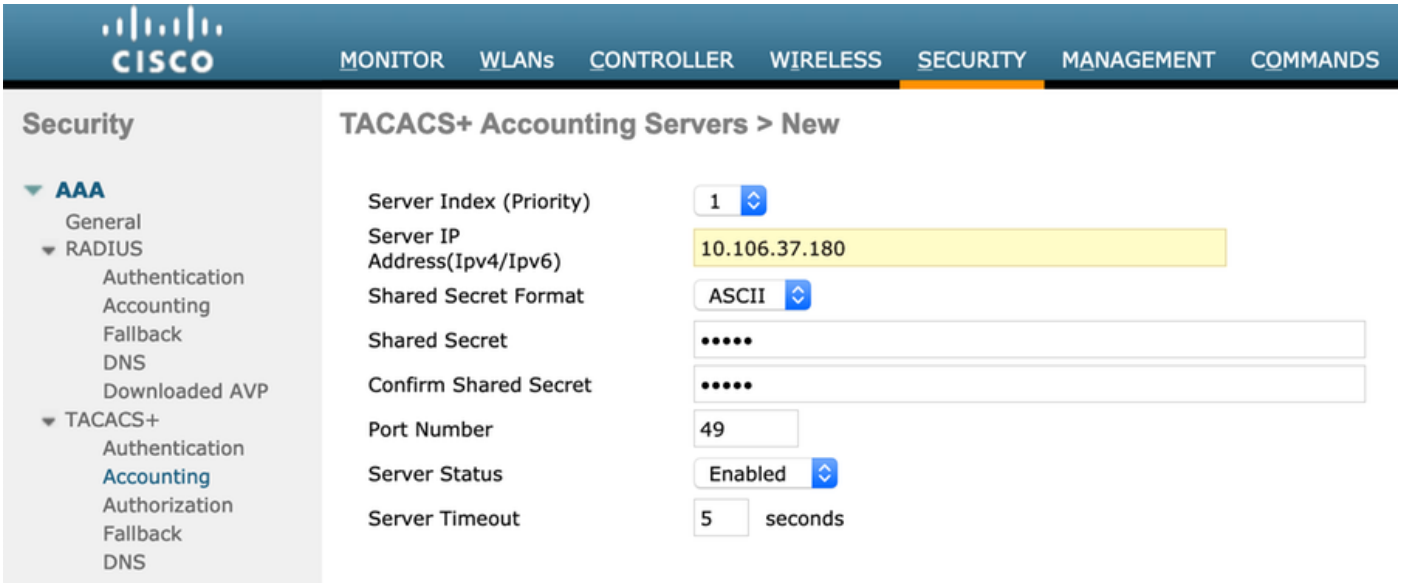
Crie duas políticas de autorização, como mostrado na imagem:



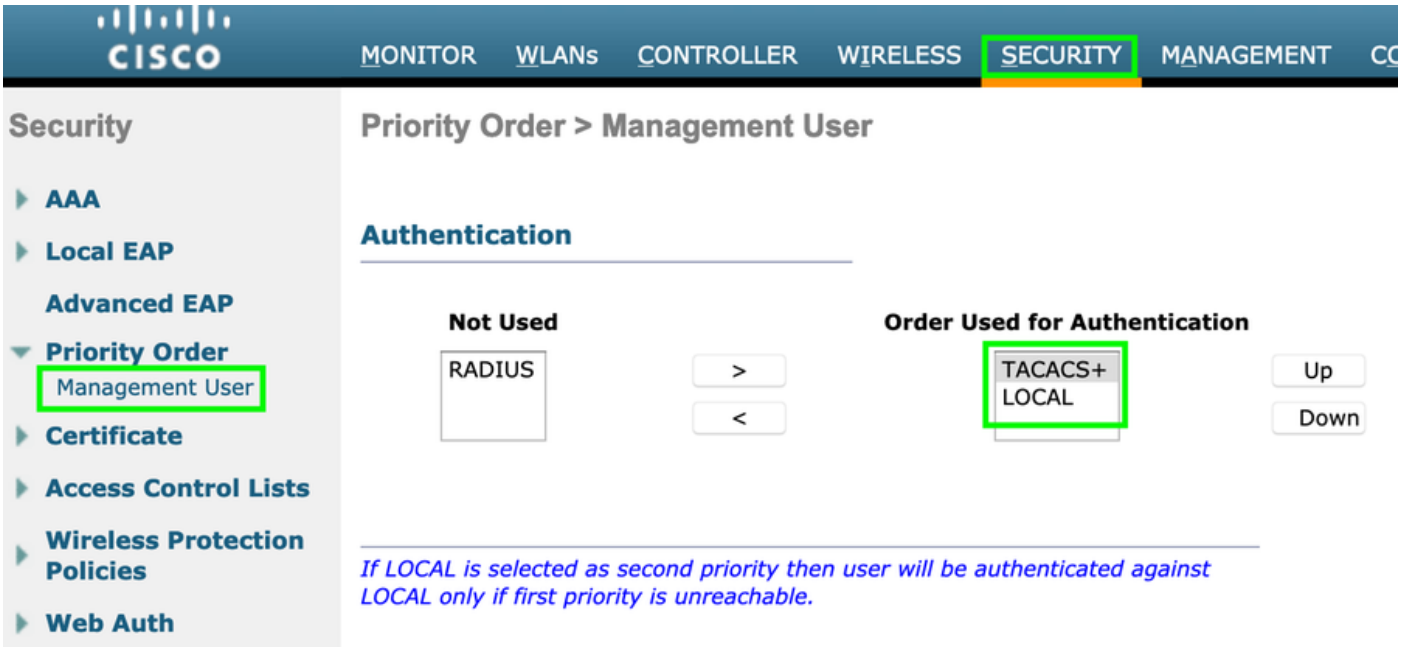
Etapa 8. Configurar o WLC para a administração do dispositivo.

Navegue até **Security > AAA > TACACS+** clique em **New** e adicione Authentication, Accounting server, como mostrado na imagem.





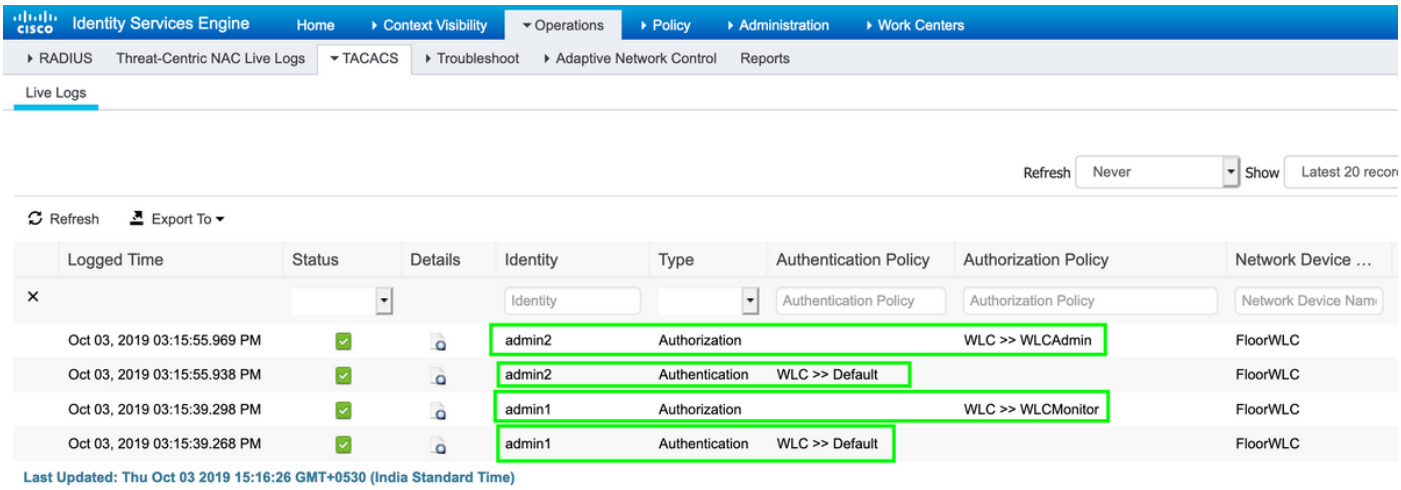
Altere a ordem de prioridade e faça TACACS+ na parte superior e Local para baixo, como mostrado na imagem:



Caution: Não feche a sessão atual da GUI do WLC. Recomenda-se abrir a GUI do WLC em diferentes navegadores da Web e verificar se o login com credenciais TACACS+ funciona ou não. Caso contrário, verifique a configuração e a conectividade com o nó ISE na porta TCP 49.

Verificar

Navegue até **Operations > TACACS > Live logs** e monitore os **Live Logs**. Abra a GUI do WLC e faça login com as credenciais do usuário do Ative Diretory, como mostrado na imagem



Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.